and 15 as obvious over the Hashimoto U.S. Patent, in view of Lillibridge U.S. Patent 6,195,698. In the TV mail system of the Hashimoto patent (see Fig. 1), a Center Response Server 30 receives email sent to a user's email address and places it in the Receiver Mail Box 36 from which a Mail Distribution Program routes it to the user's Mail Box 37. A Mail Transfer Program 33 of the Center Response Server 30 communicates with a Local Response Server 20 which operates a Client Program 22 that communicates with the Program Controller 12 of an Interactive Television Unit 10 for displaying email to the user on the TV screen.

In the comments to the rejection, the Examiner essentially takes the position that the Hashimoto Center Response Server 30 reads on Applicant's claimed "email rejection module operable with the senders list module", and the Hashimoto Local Response Server 20 reads on Applicant's email receiving server. However, even if the Hashimoto Center Response Server 30 is taken to be an "email rejection module", the limitation in the Applicant's main Claims 1, 13, and 18 of "enabling the email receiving server to send an error message back to the email sending server that the email ... is not accepted by the email receiving server" is not deemed to be fully met by Hashimoto. In the Hashimoto disclosure, the Center Response Server 30 clearly acts to receive the email and place it in the Receiver Mail Box 36, from which a decision is made whether to distribute it to the Local Response Server 20 depending on whether the sender is authorized to send email to the recipient. The Mail Distribution Program 39 requests a Name Analysis Server Program 38 to determine if the sender ID is on the authorized sender list, and if it is not, then "present mail data is abolished and abolition is notified to the sender" (Col. 12, Lines 62-67, and Col. 13, Lines 1-4).

A fundamental difference is evident between Hashimoto's invention and the Applicant's in that Hashimoto teaches to receive the email first and then decide on whether or not to abolish it. This approach applies to both his "authorized sender's list" and "rejected sender list". Hashmoto's invention must receive the email in order to decide on what to do with it because his mail data includes both the destination header and the body in a single structure. The received email is then either transmitted in a single step (Figs. 8, 9, 21, 33, 35, 51, & 56) to the Local Response Server or abolished (deleted) if not accepted by the Local Response Server. Hashimoto teaches that the step of deciding to abolish the email contents is performed after the

step of receiving the email. The fact that Hashimoto requires the step of "abolishing" the email if not accepted by the Local Response Server and then sending a notice of the deletion to the sender makes it evident that the full email has already been received. Hashimoto also states explicitly (in col. 10, lines 19-28) that "the mail data [has] ... the sending format shown in Fig. 7", which shows the mail data as including the destination header and the email text body.

The Hashimoto approach differs significantly from the Applicant's invention in which, if an email is to be rejected, it is done so before it is accepted, and therefore it is never received. This is achieved in the present invention using the procedure required in the standard email-sending protocol (SMTP): (1) the sending server sends a request to transmit email identifying the sender and receiver email addresses to the receiving server; and (2) if the receiving server accepts, then the sending server transmits the actual email. The present invention takes advantage of this protocol to make the decision to reject unauthorized email before the actual email is accepted from the sending server.

The present invention cannot be deemed obvious by one versed in the art upon reviewing Hashimoto's teaching, primarily because Hashimoto teaches screening the email in a transfer process to the receiving server after the email has already been received by the response server. His invention would have to be significantly redesigned with hindsight reconstruction in order to analyze the sender name and reject non-authorized email before it is sent by the sending server.

Hashimoto cannot accomplish the effect obtained in the present invention in which the email is never accepted and a system error message is sent back to the email sending server (typically, "550 Error, Unknown user") which will deter the sender from continuing to spam the recipient's email address. In Hashimoto, since the email is received, the spammer, especially if it is operated as an automated program, would ignore the recipient's message of deletion and continue to spam the recipient's email address. In contrast, the Applicant's system error message would be recognized by an automated spam program as a system response of an invalid email address, and would typically result in removal of the invalid address from the spammer list.

In order to define the difference between the present invention and the Hashimoto teachings even more clearly, Claims 1-20 are cancelled, and new Claims 21- 40 in method format are submitted reciting the email sending protocol sequence between the sending server and the receiving server that results in a system error message of non-acceptance of non-authorized email. The new Claims 21 – 40 now clearly define an email non-acceptance procedure which is distinct from Hashimoto. Claims 21-31 define the method in terms of checking the ASL list for authorized senders, Claims 32-39 define checking the ASL list for non-authorized senders, and Claim 40 in "means for" format defines checking the ASL list to determine if a sender is authorized or not. In view of the advantages provided in the invention of using the system error message for non-authorized senders to "trick" the sending server into "thinking" it has an unrecognized recipient address and removing it from its spammer list, the claimed invention should be considered as patentably distinct from Hashimoto which did not recognize this approach and its attendant advantages.

Moreover, depending Claims 24-27 and 35 – 36 define the procedure for confirming rejected senders as authorized senders and updating the ASL lists with confirmed authorized senders by redirecting rejected senders to the WBM website and having them validate themselves in the WBM human performance test. This WBM validation function is not described or suggested in the Hashimoto reference. While Lillibridge discloses a website procedure for validating if a user is human (as opposed to an automated program), neither Hashimoto nor Lillibridge contains any disclosure or suggestion to use the human performance procedure to confirm rejected email senders as authorized email senders, and to incorporate confirmed authorized senders on the ASL lists.

Depending Claims 28 - 30 and 37-38 further define the ASL updating function wherein various analysis rules are used to analyze the addresses of email sent by the user and website addresses accessed by the user to automatically update the ASL with authorized sender names. The automatic name analyses functions of the ASL are now recited as dependent on automated address capture. In contrast, Hashimoto uses name analysis to display the sender name and address to the recipient for approving receipt of email, not to automatically evaluate

the user's own email-sending or website accessing history for automatic additions of authorized sender names to the ASL.

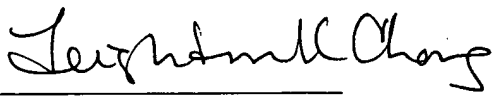
In summary, Claims 21 - 40 as amended are deemed to be patentably distinct over the cited prior art and in condition for allowance, and it is requested that a Notice of Allowance be issued therefor upon reconsideration.

This response is filed with total and independent claims after amendment numbering within the limits originally paid for with the filing fee. However, if any fees are deemed to be due for acceptance of this response, authorization is hereby given to charge our Deposit Account No. 502633.

CERTIFICATE OF MAILING:

The undersigned certifies that the foregoing is being mailed on April 29, 2004, by depositing it with the U.S. Postal Service, first class postage prepaid, addressed to: Mail Stop: RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Respectfully submitted,
ATTORNEYS FOR APPLICANT



Leighton K. Chong
USPTO Reg. No. 27,621
OSTRAGER CHONG & FLAHERTY (HAWAII)
841 Bishop Street, Suite 1200
Honolulu, HI 96813-3908
Tel: (808) 533-4300
(HST 6 hrs < EST)

AMENDMENT OF CLAIMS

(Claims 1-20, cancelled)

(Claim 21, newly added)

21. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) of email addresses of external users authorized to send email to the user,

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list; and

(e) if the sender address of the intended email is recognized as being on the user's ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not recognized as being on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server that the email-receiving server will not accept the sending of the email to the email-receiving server.

(Claim 22, newly added)

22. A method according to Claim 21, wherein the ASL module includes an ASL database

for storing ASL lists of authorized sender addresses for respective users of the email-receiving server, a spam processor module for checking the ASL lists for matches, and an ASL manager for creating, maintaining, and updating the ASL lists.

(Claim 23, newly added)

23. A method according to Claim 21, wherein a redirector module is provided to operate with the ASL module for receiving the message from the email-sending server requesting to send email designating the sender's FROM address and intended recipient's TO address, for sending a request for validation to the spam processor module to determine whether the sender's FROM address matches any authorized sender address maintained on the ASL list corresponding to the TO address of the intended recipient, for sending the reply message accepting the email from the email-sending server if a match to an authorized sender address is found, and for sending the error message not accepting the email if no match to an authorized sender address is found on the ASL list.

(Claim 24, newly added)

24. A method according to Claim 23, wherein a web-based messaging (WBM) module is provided to which the sender of intended email that is not accepted by the email-receiving server is redirected by the redirector module, and wherein the WBM module sends a message to the address of the sender of the non-accepted email notifying the sender to confirm with the WBM module that the sender is a legitimate sender of email to the intended recipient.

(Claim 25, newly added)

25. A method according to Claim 24, wherein the WBM module is a website accessible on the network which invites the notified sender to log on and confirm that the sender is a legitimate sender of email through an interaction procedure which can only be performed by a human.

(Claim 26, newly added)

26. A method according to Claim 25, wherein the interaction procedure includes a display of a graphic image of a word in a non-standard font, and a prompt to the sender to enter in a word corresponding to the graphic image of the word, whereby the system can confirm that the interaction procedure is not performed by a mechanical program.

(Claim 27, newly added)

27. A method according to Claim 24, wherein once the sender is confirmed as a legitimate sender of email to the intended recipient user, the WBM website sends a message to the redirector module at the user's email-receiving server that the sender is confirmed as a legitimate sender by the WBM website.

(Claim 28, newly added)

28. A method according to Claim 22, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis.

(Claim 29, newly added)

29. A method according to Claim 28, wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined address capture rules for updating the ASL lists using data from an email address source selected from the group of email address sources consisting of: received email; sent email; user inputs to email service functions on the email client; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

(Claim 30, newly added)

30. A method according to Claim 28, wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined analysis rules for updating the ASL lists using data from an analysis source selected from the group of analysis sources consisting of: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

(Claim 31, newly added)

31. A method according to Claim 22, wherein the ASL manager maintains the ASL lists to designate a sender-address status for each sender address selected from the group of sender-address statuses consisting of: always authorized as a friend; authorized as a friend over a date range;

authorized as a friend before an expiration date; always rejected as a spammer; rejected as a spammer matching a black list; and rejected as a spammer sent with an error message.

(Claim 32, newly added)

32. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) which identifies email addresses of external users not authorized to send email to the user;

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list of external users not authorized to send email to the user; and

(e) if the sender address of the intended email is recognized as being authorized on the user's ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is recognized as being not authorized on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server that the email-receiving server will not accept the sending of the email to the email-receiving server.

(Claim 33, newly added)

33. A method according to Claim 32, wherein the ASL module includes an ASL database for storing ASL lists of both authorized and non-authorized sender addresses for respective users of the email-receiving server, a spam processor module for checking the ASL lists for matches, and an

ASL manager for creating, maintaining, and updating the ASL lists.

(Claim 34, newly added)

34. A method according to Claim 32, wherein a redirector module is provided to operate with the ASL module for receiving the message from the email-sending server requesting to send email designating the sender's FROM address and intended recipient's TO address, for sending a request for validation to the spam processor module to determine whether the sender's FROM address matches any authorized sender address maintained on the ASL list corresponding to the TO address of the intended recipient, for sending the reply message accepting the email from the email-sending server if a match to an authorized sender address is found, and for sending an error message not accepting the email if no match to an authorized sender address is found on the ASL list.

(Claim 35, newly added)

35. A method according to Claim 34, wherein a web-based messaging (WBM) module is provided to which the sender of intended email that is not accepted by the email-receiving server is redirected by the redirector module, and wherein the WBM module sends a message to the address of the sender of the non-accepted email notifying the sender to confirm with the WBM module that the sender is a legitimate sender of email to the intended recipient.

(Claim 36, newly added)

36. A method according to Claim 35, wherein once the sender is confirmed as a legitimate sender of email to the intended recipient user, the WBM website sends a message to the redirector module at the user's email-receiving server that the sender is confirmed as a legitimate sender by the WBM website.

(Claim 37, newly added)

37. A method according to Claim 33, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis, and wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined address capture rules for updating the ASL lists using data from an email address source selected

from the group of email address sources consisting of: received email; sent email; user inputs to email service functions on the email client; inputs from user browsing of web sites; user desktop organizer and other contact lists; and third party address program inputs.

(Claim 38, newly added)

38. A method according to Claim 33, wherein email addresses used on email sent by a user which receives email through the email-receiving server and other addresses accessed by the user on the network are captured and stored with the ASL manager for later analysis, and wherein the ASL manager analyzes the captured addresses using a rules processor for processing predefined analysis rules for updating the ASL lists using data from an analysis source selected from the group of analysis sources consisting of: user email log analysis; expiration date analysis; low/high email volume analysis; fuzzy logic analysis; and third party data analysis.

(Claim 39, newly added)

39. A method according to Claim 33, wherein the ASL manager maintains the ASL lists to designate a sender-address status for each sender address selected from the group of sender-address statuses consisting of: always authorized as a friend; authorized as a friend over a date range; authorized as a friend before an expiration date; always rejected as a spammer; rejected as a spammer matching a black list; and rejected as a spammer sent with an error message.

(Claim 40, newly added)

40. A system for eliminating unauthorized email on a network comprising:

(a) first means for establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) second means for making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) for identifying which email addresses of external users are authorized to send email to the user;

(c) third means for receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is

addressed from a given sender address; and

(d) fourth means for causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list as being authorized to send email to the user;

(e) wherein, if the sender address of the intended email is recognized as being authorized on the user's ASL list, said fourth means causing the email-receiving server to send a reply message, under the common email-sending system protocol, to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not authorized on the user's ASL list, said fourth means causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server that the email-receiving server will not accept the sending of the email to the email-receiving server.